PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-214777
(43)Date of publication of application : 04.08.2000

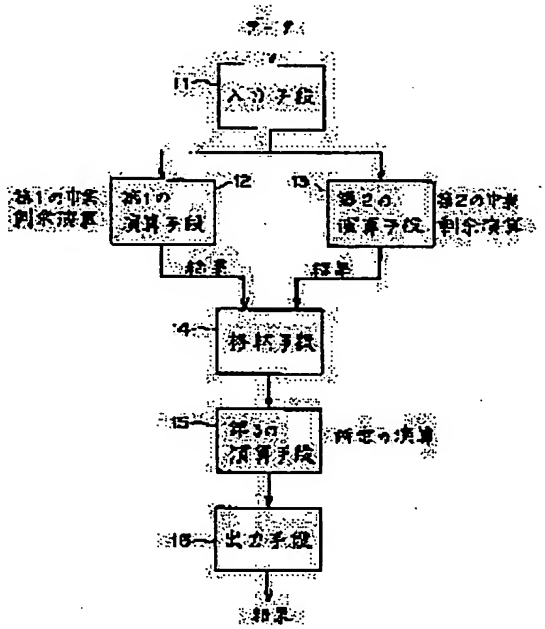
(51)Int.Cl. G09C 1/00
G06F 7/72

(21)Application number : 11-013258
(22)Date of filing : 21.01.1999

(71)Applicant : FUJITSU LTD
(72)Inventor : OKAZAKI KOTARO

(54) ARITHMETIC UNIT FOR PERFORMING WIDTH REMAINDER CALCULATION

(57)Abstract:
PROBLEM TO BE SOLVED: To execute fast calculation of width remainder utilized for a ciphering system, etc., by processing two width remainder calculations in parallel.
SOLUTION: An input means 11 inputs data to calculation means, and a calculation means 12 calculates a 1st width remainder of the input data, and a calculation means 13 calculates a 2nd width remainder of the input data in parallel with the calculation means 12. And, a storage means 14 stores the results of the 1st and 2nd width remainder calculations. After that, the results of the two width remainder calculations are taken out of the storage means 14 by a calculation means 15, and a prescribed calculation is performed, and the calculation result is outputted by an output means 16. For example, in the case of cryptograph calculations based on the remainder theorem of the Chinese, the calculation means 12, 13 execute width remainder calculations of a specified formula concerning a ciphering data in parallel, and the calculation means 15 executes calculation of a specified formula by using those calculation results.



LEGAL STATUS

[Date of request for examination] 30.11.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

Japanese Publication for Unexamined Patent Application

No. 2000-214777 (Tokukai 2000-214777)

A. Relevance of the above-identified Document

This document has relevance to claims 1, 2 and 6 to 13 of the present application.

B. Translation of the Relevant Passages of the Document

See the attached English Abstract.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－214777
(P2000－214777A)
(43)公開日　平成12年８月４日(2000.8.4)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
G09C 1/00	650	G09C 1/00	650A	5J104
	620		620A	
G06F 7/72		G06F 7/72		

審査請求　未請求　請求項の数6　OL　（全８頁）

(21)出願番号　特願平11－13258

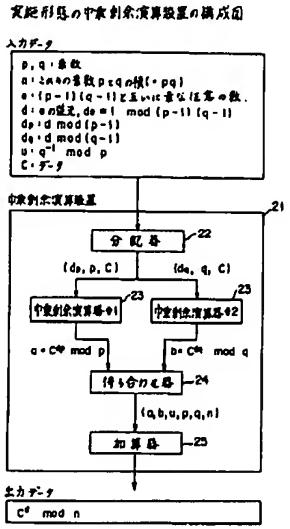
(22)出願日　平成11年１月21日(1999.1.21)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　岡崎　耕太郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100074099
弁理士　大菅　義之　（外１名）

Fターム(参考)　5J104 AA22 JA23 NA18

(54)【発明の名称】　中乗剰余演算を行う演算装置

(57)【要約】
【課題】　暗号システム等において、中乗剰余演算をより高速に実行することが課題である。
【解決手段】　分配器２２は、入力データをと２つの中乗剰余演算器２３に分配し、２つの中乗剰余演算器２３は、２つの中乗剰余演算を並行して行う。待ち合わせ器２４は、２つの中乗剰余演算の完了を待ち合わせ、加算器２５は、中国人の剰余定理に基づく加算処理を行う。



(2)

1

【特許請求の範囲】
【請求項１】　データを入力する入力手段と、
入力データに関する第１の中乗剰余演算を行う第１の演算手段と、
前記第１の演算手段と並行して、前記入力データに関する第２の中乗剰余演算を行う第２の演算手段と、
前記第１および第２の中乗剰余演算の結果を格納する格納手段と、
前記第１および第２の中乗剰余演算の結果を用いて所定の演算を行う第３の演算手段と、
前記所定の演算の結果を出力する出力手段とを備えることを特徴とする演算装置。
【請求項２】　前記入力データを前記第１および第２の演算手段に分配する分配手段と、前記第１および第２の中乗剰余演算の完了を待ち合わせる待ち合わせ手段をさらに備えることを特徴とする請求項１記載の演算装置。
【請求項３】　前記第３の演算手段は、前記第１および第２の中乗剰余演算の結果を用いた剰余演算を行って、前記所定の演算の結果を生成することを特徴とする請求項１記載の演算装置。
【請求項４】　暗号データを入力する入力手段と、
前記暗号データに関する第１の中乗剰余演算を行う第１の演算手段と、
前記第１の演算手段と並行して、前記暗号データに関する第２の中乗剰余演算を行う第２の演算手段と、
前記第１および第２の中乗剰余演算の結果を格納する格納手段と、
前記第１および第２の中乗剰余演算の結果を用いて、中国人の剰余定理に基づく演算を行う第３の演算手段と、
前記中国人の剰余定理に基づく演算の結果を出力する出力手段とを備えることを特徴とする演算装置。
【請求項５】　素数ｐおよびｑ、該素数ｐとｑの積ｎ、（ｐ－１）（ｑ－１）と互いに素な任意の数ｅ、および該任意の数ｅの逆元ｄをパラメータとして用いて、ｄを巾数としｎを法とするデータＣの中乗剰余演算を行う演算装置であって、
ｄ　ｍｏｄ（ｐ－１）を巾数としｐを法とする前記データＣの中乗剰余演算と、ｄ　ｍｏｄ（ｑ－１）を巾数としｑを法とする該データＣの中乗剰余演算を並行して行う演算手段と、
前記演算手段による２つの中乗剰余演算の完了を待って、中国人の剰余定理に基づき該２つの中乗剰余演算の結果を合成する加算手段と、
合成結果を出力する出力手段とを備えることを特徴とする演算装置。
【請求項６】　コンピュータのためのプログラムを記録＊

$$C = M^e \bmod n$$

（１）式は、ｅを巾数としｎを法とするデータＭの中乗剰余演算を表し、データＣは、M^e をｎで割ったときの剰余に対応する。

2

＊した記録媒体であって、
入力データに関する第１の中乗剰余演算と、該入力データに関する第２の中乗剰余演算を並行して行うステップと、
前記第１および第２の中乗剰余演算の結果を格納するステップと、
前記第１および第２の中乗剰余演算の結果を用いて所定の演算を行うステップとを含む処理を前記コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、安全で信頼性の高い通信ネットワークを構築するために必要な暗号システム等において用いられる演算装置に関する。
【０００２】
【従来の技術】従来より、ネットワーク上での電文秘匿、改ざん防止、および相手認証等のセキュリティを実現するために、通信データの暗号化が行われている。このような暗号化アルゴリズムは、秘密鍵暗号と公開鍵暗号に大別される。公開鍵暗号によれば、鍵の配送が不要となり、不特定多数の間での暗号通信が可能である。さらに、公開鍵暗号によりディジタル署名も可能となった。
【０００３】このような公開鍵暗号の代表的なものとして、ＲＳＡ暗号がある。このＲＳＡ暗号はオイラーの定理に基づいており、暗号化処理の流れは以下の通りである。
［１］まず、データ受信者は、以下の公開鍵および秘密鍵を用意する。
【０００４】ｐ，ｑ：素数
ｎ：これらの素数ｐとｑの積（＝ｐｑ）
ｅ：（ｐ－１）（ｑ－１）と互いに素な任意の数
ｄ：ｅの逆元、すなわち、ｄｅ≡１　ｍｏｄ（ｐ－１）（ｑ－１）
ここで、（ｅ，ｎ）が公開鍵に対応し、ｄが秘密鍵に対応する。また、ｄｅ≡１ｍｏｄ（ｐ－１）（ｑ－１）は、合同式と呼ばれ、左辺（＝ｄｅ）および右辺（＝１）を（ｐ－１）（ｑ－１）で割ったときの剰余が一致することを表している。
［２］次に、データ受信者は、公開鍵（ｅ，ｎ）を公開する。
［３］次に、データ送信者は、送信するデータ（平文）Ｍ（＜ｎ）を、データ受信者が公開した公開鍵を使って、以下のように暗号化する。

$$C = M^e \bmod n \quad (1)$$

［４］次に、データ送信者は、公開鍵を使って暗号化されたデータＣ（＜ｎ）を、公開鍵を公開したデータ受信者に送付する。

[5] 次に、公開鍵を使って暗号化されたデータCを受信したデータ受信者は、それを秘密鍵を使って以下の式で復号化する。

$$P=C^d \bmod n \quad (2)$$

(2) 式は、dを巾数としnを法とするデータCの巾乗剰余演算を表す。データ送信者が正しい公開鍵を使用して暗号化したデータを送付した場合、$P=M^{ed} \bmod n=M$となる。

【0005】このRSA暗号処理の流れにおいて、データ送信者が公開鍵を使って (1) 式の巾乗剰余演算を行う場合、公開鍵eとしては一般的に小さく、かつ、高速に巾乗剰余演算が可能な値（例えば、$2^{16}+1$）が使用されるため、その巾乗剰余演算を比較的高速に行うことが可能である。

※うに復号化する。

※【0006】しかし、データ受信者が秘密鍵を使って (2) 式の巾乗剰余演算を行う場合、秘密鍵は大きな値であるため、その巾乗剰余演算の計算量は大きなものとなる。そこで、一般的には、以下に紹介する中国人の剰余定理を用いて、(2) 式の巾乗剰余演算に要する時間の削減が行われている。

【中国人の剰余定理】m_i (i=1, 2, . . . , r) を互いに素な正の整数とし、a_i (i=1, 2, . . . , r) を正の整数とすると、r個の連立合同式

$$x=a_i \bmod m_i \quad (i=1, 2, \ldots, r) \quad (3)$$

は、$M=\Pi m_i$ を法とする一意な解を持ち、その解は、

★式で与えられる。

$$x=\Sigma a_i M_i y_i \bmod M \quad (4)$$

ただし、i=1, 2, . . . , rに対して、

$$M_i=M/m_i,\ y_i=M_i^{-1} \bmod m_i \quad (5)$$

である。

☆【中国人の剰余定理】(r=2)

p, qを互いに素な正の整数とし、a, bを整数とする。このとき、

【0007】ここで、r=2とすると、上述の中国人の剰余定理は次のように書き換えられる。

☆

$$x=a \bmod p, \quad (6)$$

$$x=b \bmod q \quad (7)$$

を満たすx (<pq) が唯一存在し、

$$x=(a-b)(q^{-1} \bmod p)q+b \quad (8)$$

となる。この中国人の剰余定理を使用することにより、(2) 式の巾乗剰余演算を以下のようにして行うことができる。[1] まず、データ受信者は、以下のパラメータを用意する。

【0008】p, q：素数

n：これらの素数pとqの積 (=pq)

e：(p−1) (q−1) と互いに素な任意の数

d：eの逆元、すなわち、$de \equiv 1 \bmod (p-1)$

◆$d_p : d \bmod (p-1)$

$d_q : d \bmod (q-1)$

$u : q^{-1} \bmod p$

データ受信者は、素数p, qを認識しているため、これらの値をデータを受信する前にあらかじめ用意しておくことが可能である。[2] 次に、データ受信者は、データCを受信し、次式を計算する。

$$a=C^{dp} \bmod p \quad (9)$$

(9) 式は、d_p を巾数としpを法とするデータCの巾乗剰余演算を表す。[3] さらに、データ受信者は、次式を計算する。

$$b=C^{dq} \bmod q \quad (10)$$

(10) 式は、d_q を巾数としqを法とするデータCの巾乗剰余演算を表す。[4] 最後に、データ受信者は、※

※ (9) 式のaと (10) 式のbを用いて、次式を計算する。

$a \geq b$なら、

$$x=((a-(b \bmod p))u \bmod p)q+b \bmod n \quad (11)$$

$a<b$なら、

$$x=((a+p-(b \bmod p))u \bmod p)q+b \bmod n \quad (12)$$

(11) 式および (12) 式はともに、pとnを法とする剰余演算を含んでおり、得られたxは (2) 式の$C^d \bmod n$と一致する。

【0009】図7は、この中国人の剰余定理を用いた従来の巾乗剰余演算装置の構成図である。図7の巾乗剰余演算装置1は、巾乗剰余演算器2と加算器3を備え、上述の [2] ～ [4] の処理を順に行う。

【0010】演算装置1には、上述したパラメータp、q、n、e、d、d_p、d_q、およびuの他に受信データCが入力データとして入力される。演算装置1は、まず、受け取った入力データからデータの組 (d_p, p, C) を生成し、巾乗剰余演算器2に渡す。そして、巾乗剰余演算器2は、受け取ったデータをもとに (9) 式の巾乗剰余演算を行い、その結果を返す。

【0011】次に、演算装置1は、受け取った入力データからデータの組 (d_q, q, C) を生成し、巾乗剰余演算器2に渡す。そして、巾乗剰余演算器2は、受け取ったデータをもとに (10) 式の巾乗剰余演算を行い、その結果を返す。

【0012】次に、演算装置1は、データの組 (a, b, u, p, q, n) を加算器3に渡す。そして、加算器3は、受け取ったデータをもとに (11) 式または (12) 式の演算を行う。最後に、演算装置1は、得られたxの値を (2) 式の$C^d \bmod n$の演算結果として出力する。

【0013】

【発明が解決しようとする課題】しかしながら、上述した従来の巾乗剰余演算装置には次のような問題がある。

【0014】RSA暗号の安全性は、公開鍵nの因数分解の難しさに基づいているが、パーソナルコンピュータ等の演算速度の向上に伴い、因数分解の処理時間が短縮される傾向にある。このため、安全性を確保するには、公開鍵nとして、よりビット数の大きな値を用いる必要があり、復号化のための巾乗剰余演算においてもより多くの計算量が要求される。

【0015】ところで、従来の巾乗剰余演算装置では、全体の処理時間のうち (9) 式および (10) 式の巾乗剰余演算の時間が大半を占めており、公開鍵nのビット数が大きくなれば、演算時間はさらに増大する。そこで、この巾乗剰余演算の処理時間を改善することが望まれる。

【0016】本発明の課題は、暗号システム等において利用される巾乗剰余演算をより高速に実行する演算装置を提供することである。

【0017】

【課題を解決するための手段】図1は、本発明の演算装置の原理図である。図1の演算装置は、入力手段11、第1の演算手段12、第2の演算手段13、格納手段14、第3の演算手段15、および出力手段16を備える。

【0018】入力手段11は、入力を入力し、演算手段12は、入力データに関する第1の巾乗剰余演算を行い、演算手段13は、演算手段12と並行して、入力データに関する第2の巾乗剰余演算を行う。そして、格納手段14は、第1および第2の巾乗剰余演算の結果を格納し、演算手段15は、第1および第2の巾乗剰余演算の結果を用いて所定の演算を行い、出力手段16は、所定の演算の結果を出力する。

【0019】このような演算装置によれば、演算手段12および13により、2つの巾乗剰余演算が並行して行われ、それらの演算結果が、一旦、格納手段14に格納される。その後、演算手段15により、2つの巾乗剰余演算の結果が格納手段14から取り出され、所定の演算が行われて、出力手段16により、その演算結果が出力される。

【0020】前述の中国人の剰余定理に基づく暗号演算の場合、演算手段12および13は、暗号データCに関する (9) 式および (10) 式の巾乗剰余演算を並行して行い、演算手段15は、それらの演算結果を用いて (11) 式または (12) 式の演算を行う。このように、2つの巾乗剰余演算を並行して処理することで、(2) 式の巾乗剰余演算の結果を高速に得ることができる。

【0021】例えば、図1の入力手段11は、後述する図5のネットワーク接続装置37に対応し、図1の格納手段14は、図5のメモリ32に対応し、図1の出力手段16は、図5の出力装置34に対応する。また、例えば、図1の演算手段12および13は、後述する図2の巾乗剰余演算器23に対応し、図1の演算手段15は、図2の加算器25に対応する。

【0022】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。

【0023】中国人の剰余定理に基づく巾乗剰余演算において、(9) 式の演算$C^{dp} \bmod p$と (10) 式の演算$C^{dq} \bmod q$の間には依存性がなく、それぞれ独立して実行することが可能である。そこで、本実施形態においては、分配器と2つの巾乗剰余演算器を用いて、これらの2つの巾乗剰余演算を並行して行う。そして、待ち合わせ器を用いて、2つの巾乗剰余演算の完了を待ち合わせ、加算器を用いて、中国人の剰余定理に基づく加算処理を行う。2つの巾乗剰余演算を並行に処理することで、処理速度が向上する。

【0024】図2は、このような巾乗剰余演算装置の構成図である。図2の演算装置21は、分配器22、2つの巾乗剰余演算器23 (#1, #2)、待ち合わせ器24、および加算器25を備える。

【0025】演算装置1には、上述したパラメータp、q、n、e、d、d_p、d_q、およびuと、受信データCとが、入力データとして入力される。演算装置1は、まず、受け取った入力データを分配器22に渡す。

【0026】分配器22は、図3に示すように、受け取った入力データから2つのデータの組 (d_p, p, C) および (d_q, q, C) を生成し、それぞれのデータの組を入力として巾乗剰余演算器#1および#2に演算を同時に依頼する。ここでは、巾乗剰余演算器#1に演算$C^{dp} \bmod p$を依頼し、巾乗剰余演算器#2に演算$C^{dq} \bmod q$を依頼する。

【0027】巾乗剰余演算器#1および#2は、それぞれが受け取ったデータをもとに、互いに独立して巾乗剰

余演算a＝C^{dp} mod pおよびb＝C^{dq} mod qを並行して行い、それぞれの演算が完了した時点で、待ち合わせ器２４に完了を通知する。このとき、中乗剰余演算器＃１から送られる完了通知には演算結果aが含まれており、中乗剰余演算器＃２から送られる完了通知には、演算結果bが含まれている。

【００２８】待ち合わせ器２４は、中乗剰余演算器＃１および＃２からの完了通知を待ち合わせた後、データの組（a，b，u，p，q，n）を生成して加算器２５に渡す。そして、加算器２５は、受け取ったデータの組（a，b，u，p，q，n）をもとに、aとbの大小関係に応じて（１１）式または（１２）式の演算を行う。最後に、演算装置２１は、得られたxの値を（２）式のC^{d} mod nの演算結果として出力する。

【００２９】このような演算装置２１によれば、２つの中乗剰余演算a＝C^{dp}mod pとb＝C^{dq} mod qが並行して処理される。ＲＳＡ暗号処理においては、十分な安全性を確保するために、pとqが極端に異ならないように決められていることが多く、その結果、これらの２つの中乗剰余演算の計算量は同じ程度になる。このため、２つの中乗剰余演算を並行して行えば、処理時間を従来の約半分に削減することが可能である。

【００３０】また、演算装置２１は、（９）～（１２）式に示した中国人の剰余定理に基づく中乗剰余演算のみならず、並行処理可能な２つの中乗剰余演算を含む任意の演算を行うことができる。この場合、加算器２５は、必要に応じて、他の演算器等に置き換えてもよい。

【００３１】図４は、待ち合わせ器２４が行う処理のフローチャートである。待ち合わせ器２４は、まず、中乗剰余演算器＃１または＃２からの完了通知を待ち合わせ、定期的に完了通知を受信したかどうかを判定する（ステップＳ１）。完了通知を受信していなければ判定を繰り返し、完了通知を受信すると、それが中乗剰余演算器＃１からのものかどうかを判定する（ステップＳ２）。

【００３２】中乗剰余演算器＃１から完了通知を受け取った場合、次に、中乗剰余演算器＃２から既に完了通知を受信しているかどうかを確認する（ステップＳ３）。ここで、中乗剰余演算器＃２からの完了通知を受信済の場合は、２つの中乗剰余演算器の演算が完了したことになる。そこで、加算器２５を呼び出して、データの組（a，b，u，p，q，n）を渡し（ステップＳ４）、処理を終了する。中乗剰余演算器＃２からの完了通知を受信していない場合は、ステップＳ１の処理を行って、その完了通知を待つ。

【００３３】ステップＳ２において、受け取った完了通知が中乗剰余演算器＃２からのものである場合、次に、中乗剰余演算器＃１から既に完了通知を受信しているかどうかを確認する（ステップＳ５）。ここで、中乗剰余演算器＃１からの完了通知を受信済の場合は、２つの中乗剰余演算器の演算が完了したことになる。そこで、ステップＳ４の処理を行って、処理を終了する。中乗剰余演算器＃１からの完了通知を受信していない場合は、ステップＳ１の処理を行って、その完了通知を待つ。

【００３４】このような待ち合わせ器２４を設けることで、中乗剰余演算器＃１および＃２の演算が終了した後、２つの演算結果を合わせて直ちに加算器２５に入力することができる。したがって、必要最小限の待ち合わせ時間の後、加算器２５の処理を開始することができる。

【００３５】図２の演算装置２１において、分配器２２、中乗剰余演算器２３、待ち合わせ器２４、および加算器２５は、それぞれ、任意のハードウェアまたはソフトウェアにより実現することができる。特に、２つの中乗剰余演算器２３としては、中乗剰余演算専用の２つのＩＣ（integrated circuit）チップ（演算専用プロセッサ）を用いてもよく、並行して動作するデュアルＣＰＵ（中央処理装置）を搭載したコンピュータの場合、各ＣＰＵに各中乗剰余演算器２３の処理を行わせることもできる。

【００３６】図２の演算装置２１は、例えば、図５に示すような情報処理装置（コンピュータ）を用いて構成することができる。図５の情報処理装置は、ＣＰＵ３１、メモリ３２、入力装置３３、出力装置３４、外部記憶装置３５、媒体駆動装置３６、ネットワーク接続装置３７、および２つの演算専用プロセッサ３８（＃１，＃２）を備え、それらはバス３９により互いに接続されている。

【００３７】メモリ３２は、例えば、ＲＯＭ（read only memory）、ＲＡＭ（random access memory）等を含み、処理に用いられるプログラムとデータを格納する。ＣＰＵ３１は、メモリ３２を利用してプログラムを実行することにより、必要な処理を行う。

【００３８】この場合、図２の分配器２２、待ち合わせ器２４、および加算器２５は、メモリ３２の特定のプログラムコードセグメントに格納されたソフトウェアコンポーネントに対応する。

【００３９】入力装置３３は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、ユーザからの指示や情報の入力に用いられる。出力装置３４は、例えば、ディスプレイ、プリンタ等であり、ユーザへの問い合わせや処理結果の出力に用いられる。

【００４０】外部記憶装置３５は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク（magneto-optical disk）装置等である。この外部記憶装置３５に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ３２にロードして使用することもできる。

【００４１】媒体駆動装置３６は、可搬記録媒体４０を駆動し、その記録内容にアクセスする。可搬記録媒体４０としては、メモリカード、フロッピーディスク、ＣＤ－ＲＯＭ（compact disk read only memory）、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。この可搬記録媒体４０に上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ３２にロードして使用することもできる。

【００４２】ネットワーク接続装置３７は、任意のネットワーク（回線）を介してデータ送信者の装置と通信し、暗号化されたデータＣを受信する。また、必要に応じて、上述のプログラムとデータを外部の装置から受け取り、それらをメモリ３２にロードして使用することもできる。

【００４３】演算専用プロセッサ＃１および＃２は、図２の中乗剰余演算器＃１および＃２に対応し、それぞれ、与えられたデータの組をもとに中乗剰余演算を行って、演算結果をメモリ３２に格納する。

【００４４】図６は、図５の情報処理装置にプログラムとデータを供給することのできるコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体４０や外部のデータベース４１に保存されたプログラムとデータは、メモリ３２にロードされる。そして、ＣＰＵ３１は、そのデータを用いてそのプログラムを実行し、必要な処理を行う。

【００４５】

【発明の効果】本発明によれば、２つの中乗剰余演算を並行に処理することが可能となり、中国人の剰余定理に見られるような複雑な中乗剰余演算を高速化することができる。これにより、例えば、公開鍵暗号のデータ受信者が秘密鍵を用いて行う中乗剰余演算の処理時間が削減される。

【図面の簡単な説明】

【図１】本発明の演算装置の原理図である。

【図２】実施形態の中乗剰余演算装置の構成図である。

【図３】分配器と中乗剰余演算器の処理を示す図である。

【図４】待ち合わせ器の処理のフローチャートである。

【図５】情報処理装置の構成図である。

【図６】記録媒体を示す図である。

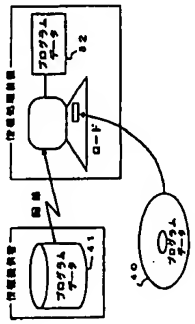
【図７】従来の中乗剰余演算装置の構成図である。

【符号の説明】

１、２１　中乗剰余演算装置
２、２３　中乗剰余演算器
３、２５　加算器
１１　入力手段
１２、１３、１５　演算手段
１４　格納手段
１６　出力手段
２２　分配器
２４　待ち合わせ器
３１　ＣＰＵ
３２　メモリ
３３　入力装置
３４　出力装置
３５　外部記憶装置
３６　媒体駆動装置
３７　ネットワーク接続装置
３８　演算専用プロセッサ
３９　バス
４０　可搬記録媒体
４１　データベース

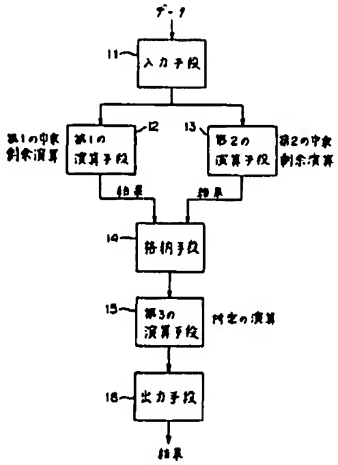
【図６】

記録媒体を示す図



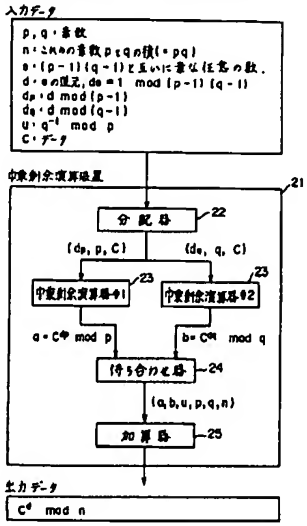
【図1】

本発明の原理図



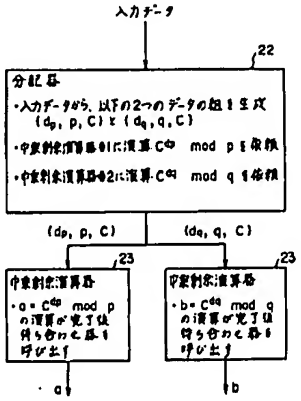
【図2】

実施形態の中剰余演算装置の構成図



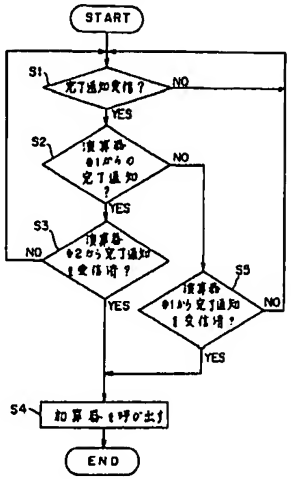
【図3】

分配器と中剰余演算器の処理を示す図



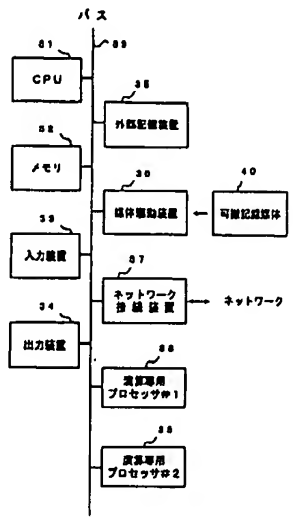
【図4】

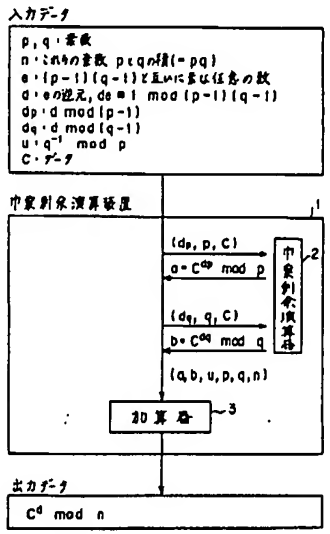
待ち合わせ器の処理のフローチャート



【図5】

情報処理装置の構成図



【図7】

従来の中剰余演算装置の構成図